EO/US
PCT/BY99/00005

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing:
02 November 2000 (02.11.00)

International application No.:
PCT/BY99/00005

Applicant's or agent's file reference:

International filing date:
27 April 1999 (27.04.99)

Priority date:

Applicant:
MISCHENKO, Valentin Alexandrovich et al

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International preliminary Examining Authority on:

11 January 2000 (11.01.00)

□ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was
□ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

14

Applicant's or agent's file reference i990186	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/BY99/00005	International filing date *(day/month/year)* 27/04/1999	Priority date *(day/month/year)* 27/04/1999
International Patent Classification (IPC) or national classification and IPC H04L9/06		
Applicant MISCHENKO, Valentin Alexandrovich et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 9 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:

   I ☒ Basis of the report
   II ☐ Priority
   III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   IV ☐ Lack of unity of invention
   V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   VI ☐ Certain documents cited
   VII ☒ Certain defects in the international application
   VIII ☒ Certain observations on the international application

Date of submission of the demand 11/01/2000	Date of completion of this report 26.07.2001
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tx: 523656 epmu d	Authorized officer Snell, T

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:

Description, pages:

1-14 as originally filed

Claims, No.:

1-11 with telefax of 10/06/2000

Drawings, sheets:

1/2,2/2 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

□ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).

□ the language of publication of the international application (under Rule 48.3(b)).

□ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

□ contained in the international application in written form.

□ filed together with the international application in computer readable form.

□ furnished subsequently to this Authority in written form.

□ furnished subsequently to this Authority in computer readable form.

□ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

□ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

□ the description, pages:

□ the claims, Nos.:

□ the drawings, sheets:

5. □ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

□ the entire international application.

☒ claims Nos. 1-5,7-10.

because:

☒ the said international application, or the said claims Nos. 1-5, 7-10 relate to the following subject matter which does not require an international preliminary examination (*specify*):
see separate sheet

□ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. are so unclear that no meaningful opinion could be formed (*specify*):

□ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

□ no international search report has been established for the said claims Nos. .

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

□ the written form has not been furnished or does not comply with the standard.

□ the computer readable form has not been furnished or does not comply with the standard.

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N) Yes: Claims 6,11

	No:	Claims	
Inventive step (IS)	Yes:	Claims	6,11
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	6,11
	No:	Claims	

2. Citations and explanations
   see **separate sheet**

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see **separate sheet**

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see **separate sheet**

Cited Document

D1: US-A-5 222 139 (TAKARAGI ET AL.) 22 June 1993 (1993-06-22)

Re Item III
Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. Claims 1-5 and 7-10 define purely mathematical steps for acting on abstract information, and thus fall within the terms of a mathematical theory for which no examination is necessary in accordance with Rule 67.1(i) PCT. Although an encryption method can be related to solving a technical problem, eg to ensure the secrecy of data transmitted via a communications system, such a method can only be patentable when embedded in a technical system, eg "a method for transferring data via a communications system, comprising encoding the data prior to transfer, the encoding comprising the steps of: ...." (cf Decision T 208/84 (Vicom) of the Board of Appeal of the European Patent Office, points 5-7 of the reasons for the decision). Any amendment however would clearly have to be based on the application documents as originally filed (eg on page 1, lines 9-11 of the description).

Re Item V
Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Claim 6 relates to a device for performing an encryption operation, and claim 11 to a device for performing a decryption operation.

   Although these claims are not clear (see section VIII), they are interpreted for the following opinion as implicitly comprising all the means for carrying out the method of claims 1 and 7 respectively.

2. Prior art document D1 discloses an apparatus for carrying out an encryption method, wherein the method comprises the steps of (in accordance with the

preamble of claim 1):

preliminary generation of data on a plurality of characteristic functions that transform values of all initial information of a full set of symbols into encoded data (see abstract, lines 4-5);

determining the number (n) of cycles of transforming specific initial information (col. 8, lines 42-44);

realising the cycle of transforming which comprises:

generating the feature that determines the "regularity" used for transforming the information in the current transformation cycle (col. 5, line 24 - col. 7, line 36); transforming the information using the selected regularity (col. 7, lines 37-43); repeating transformation cycles a certain number of times (col. 3, lines 9-27 and claim 2) .

3. The subject-matter of claim 6 therefore differs from the disclosure of D1 in having means for carrying out the steps:

transforming of the information in each cycle is performed in such a way that results in forming transformed information Ci and accessory information Fi; the number (n) of cycles of the transformation of the initial information is selected from the preassigned criterion, forming an encoded message consisting of two parts, one of the said parts comprising the finally transformed data and the second one comprising the accessory information array, and differs further in details defining the processing structure of the device.

In other words, the claimed method differs essentially over the prior art in that the accessory information is part of the encoded message; this appears not to be the case in D1. Moreover, it is not apparent in D1 that each cycle produces a new accessory information; in fact the cycles appear to be based always on the same algorithm determination key.

As modifying D1 to arrive at the invention would involve changing the fundamental concept underlying the encryption algorithm, such a step does not appear obvious. It is however noted that since the accessory information relates directly to the inventive concept, the independent claims must be far more specific in defining how the accessory information is produced (see section VIII).

Thus, despite the lack of clarity of claim 6 which renders it difficult to give a definitive opinion as to novelty and inventive step, it is considered for the above reasons that the subject-matter of claim 6 can provisionally be deemed to be novel and to involve an inventive step (Articles 33(1)-(3) PCT).

4. The same considerations apply to claim 11, which relates to a reciprocal decoding device (Articles 33(1)-(3) PCT).

5. If method claims 1-5 and 7-10 were embedded in a technical process as explained above in section III, such a technical process would provisionally also meet the requirements for novelty and inventive step (Articles 33(1)-(3) PCT).

<u>Re Item VII</u>
Certain defects in the international application

1. The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT). This would have been appropriate for apparatus claims 6 and 11.

2. The description should have been adapted to the new claims (Rule 5.1(a)(iii) PCT). Moreover, the numbers at the head of each paragraph on pages 5-9 should have been deleted as they create the confusing impression of being claims (Article 6 PCT).

Re Item VIII

Certain observations on the international application

1. Claims 1-11 are currently so unclear (Article 6 PCT) that the positive opinion as to novelty and inventive step given in the foregoing can only be regarded as provisional.

2. Conceming claim 1:

   (i) The meaning of the term "regularity" is somewhat obscure. Although this term has been replaced by the term "characteristic functions" in line 2 of claim 1, this has not been done throughout the claim.

   (ii) The term "generating the feature (R_i)" is broader than justified by the extent of the description and drawings, since the only example given in the description is that of a generating a random number.

   (iii) The step "transforming of the information in each cycle is performed in such a way that results ... " is defined as a goal to be achieved without defining any steps which define the actual transformation performed, which, since this relates to the inventive contribution to the art, also results in the claim not including all the essential features of the invention. The matter on page 12, lines 25-31 of the description should have been included in claim 1.

   Claim 1 therefore does not meet the requirements of Article 6 PCT.

3. Claim 7, related to a decoding process, also uses the term regularity, and contains no information on the type of transformation used. Claim 7 is therefore as equally unclear as claim 1 (Article 6 PCT).

4. Device claim 6 lacks essential features of the invention, as a structure of a device is defined, but none of the structural features are defined in terms of the function they carry out, ie the method of claim 1.

   Since an independent claim must be comprehensible by itself, claim 6 should have included, in terms of apparatus features, a clear definition of the encoding method defined in claim 1. Functional features for example may be defined as "means for ...", means adapted for ..." etc.

The same objection applies to device claim 11, which should clearly include all means necessary for carrying out the decoding method of claim 7.

Claims 6 and 11 therefore also lack clarity (Article 6 PCT).

5. A further cause of obscurity in all the claims is the frequent use of the definite article "the" to define features appearing for the first time (see in particular in claim 1 "the preassigned criterion", and the characterising portion of claim 6). Where features ave no antecedent, the indefinite article "a" should have been used (Article 6 PCT).

Claims

1. A method for encoding data comprising the steps of:

- preliminary generating data on plurality of characteristic functions that transform values of initial information of a full set of symbols into encoded data;
- determining the number (n) of cycles of transforming specific initial data;
- realising the cycle of transforming which comprises:
- generating the feature (R_i) that determines the regularity used for transforming the data in the current transformation cycle;
- transforming the data using the selected regularity;
- repeating transformation cycles a certain number of times;

- *characterised in that,*
- transforming of the data in each cycle is performed in such a way that results in forming a transformed in the said cycle data (C_i) and the accessory data for the said cycle (F_i);
- the number (n) of cycles of the transformation of the initial data is selected from the preassigned criterion,
- forming an encoded message consisting of two parts, one of the said parts comprises the finally transformed data (C_n), and the second one comprises the accessory data array ($F = \{F_1, F_2, \ldots, F_n\}$).

2. The method for encoding data according to claim 1, *characterised in that*

- transforming the data in each cycle is performed in such a way that results in forming a transformed in the said cycle data (C_i), that is shorter or equal to the length of the initial data, and the accessory data for the said cycle (F_i);
- the number (n) of cycles of the transformation of the initial data is selected from the preassigned criterion determining the size of the finally transformed data,
- forming an encoded message consisting of two parts, one of the said parts comprises the finally transformed data (C_n) that is shorter than the length of the initial communication, and the second one comprises the accessory data array ($F = \{F_1, F_2 \ldots, F_n\}$).

3. The method for encoding data according to claim 1, *characterised in that*

- transforming the data in each cycle is performed in such a way that results in forming a transformed in the said cycle data (C_i) that is shorter, equal or longer than the length of the initial data and the accessory data for the said cycle (F_i);

- the number (n) of cycles of the transformation of the initial data is selected from the preassigned criterion, determining the size of the finally transformed data and/or the degree of protectability of data.
- forming an encoded data consisting of two parts, one of the said parts comprises the finally transformed data (C_n) that is shorter, equal or longer than the length of the initial communication, and the second one comprises the accessory data array ($F = \{F_1, F_2, \ldots, F_n\}$).

4. The method according to claims 1, 2 or 3, *characterised in that* the transformed in the said cycle data (C_i) and/or the accessory data for the said cycle (F_i) are mixed in each cycle or in some cycles.

5. The method according to claims 1, 2, or 3, or 4, *characterised in that* the certain part of the accessory data for the said cycle (F_i) is added to the transformed in the said cycle data (C_i) in each or some transformation cycles.

6. The device for realising the method for encoding of data, comprises:

- an input unit,
- an output unit, the first input of which is connected with the second output of the commutator, and the second — with the output of the accessory data storage ;
- data base on the plurality of characteristic functions that transform the initial data with the encoded data, the first input of the said data base being connected with the first output of the input unit and the second input – with the output of the random numbers generator;
- *characterised in that*, the device further comprises
- a random number generator, the input of which is connected with the first output of the making decision unit;
- the transformation unit, the first input of which is connected with the second output of the output unit, the second input –with the output of the data base, and the third input –with the first output of the commutator;
- the storage for the transformed data, the input of which is connected with the first output of the transformation unit;
- a storage for the accessory data, the first input of which is connected with the second output of the transformation unit, and the second input – with the second output of the making decision unit;
- the making decision unit, the first input of which is connected with the third output of the input unit, the second input – with the first output of the storage for the transformed communication;

- the commutator, the first input of which is connected with the second output of the storage for the transformed communication, and the second input – with the second output of the making decision unit.

7. The method for decoding of the encoded data comprising the steps of:

- preliminary generating data on plurality of characteristic functions that transform values of all encoded symbols that may be used in the said kind of data with initial symbols, which are identical to the regularities used at encoding;
- extracting , from the encoded communication, of the data (R_i), defining the regularity which is used in the current transformation cycles and connects the values of the encoded communications with the concrete symbols of the transformed data of the current transformation cycle;
- selecting the regularity connecting the values of the encoded communications with the concrete symbols of the transformed data of the current transformation cycle;
- extracting from the accessory data (F) the accessory data for the said transformation cycle (F_i);
- transforming the transformed data (C_i) using the selected regularity and the accessory data for the said transformation cycle (F_i);
- making decision on switching to the next cycle or termination of the transformation;
- *characterised in that,* the accessory data for the said transformation cycle (F_i); is isolated from the array of the accessory data (F);
- recovering the data (C_i), which is transformed in the respective cycle, by using the selected regularity and the accessory data for the said transformation cycle (F_i);
- making decision on switching to the next cycle or termination of the transformation;
- using additionally in each transformation cycle a respective part of the accessory data, as a result of transforming with the use of the selected regularity there is formed the data recovered in the respective cycle.

8. The method of decoding the encoded data according to claims 7, *characterised in that*

- In each transformation cycle there is additionally used a respective part of the accessory data and as a result of transformation with use of the selected regularity there is formed a recovered in the communication, the length of which is larger or equal to the length of the communication, resulting from transforming in the previous cycle.

9. The method of decoding the encoded data according to claims 7, *characterised in that*

in each transformation cycle there is additionally used a respective part of the accessory data, and as a result of transformation with use of the selected regularity there is formed a recovered in the respective cycle communication, the length of which is larger, equal or smaller than the length of the communication, resulting from transforming in the previous cycle.

10. The method according to claims 7, 8 or 9, *characterised in that*, the transformed in the respective cycle data (C_i) and/or the accessory data for the respective cycle (F_i) is preliminary unmixed in each cycle or in some cycles;

11. The device for realising the method for decoding data, comprises:

- an input unit,
- an output unit,
- data base on the plurality of characteristic functions that transform the encoded data with the initial data,
- *characterised in that*, the device further comprises
- a transformation unit;
- a storage of the recovered communication;
- a storage of the accessory data;
- a making decision unit;
- a commutator,

the first input of the accessory data storage connected with first output of the input unit and the second input of the accessory data storage connected with first output a making decision unit; the first input of data base is connected to the second output of the of the input unit, and the second input – to the first output of the storage for accessory data; the first input of the storage of the recovered data is connected to the third output of the input unit, the second – to the output of the transformation unit, and the third – to the first output of the making decision unit, the first input of the transformation unit is connected to the second output of the storage of accessory data, and the second – to the output of database, the third to the first output of the storage of recovered data; the second - to the fourth output of the input unit, the first input of the commutator is connected to the second output of the making decision unit, and the second – to the second output of th making decision unit, the output unit is connected to the second commutator output .

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/BY 99/ 00005	International filing date *(day/month/year)* 27/04/1999	(Earliest) Priority Date *(day/month/year)*
Applicant MISCHENKO, Valentin Alexandrovich et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 2 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

□ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

□ contained in the international application in written form.

□ filed together with the international application in computer readable form.

□ furnished subsequently to this Authority in written form.

□ furnished subsequently to this Authority in computer readble form.

□ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

□ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. □ **Certain claims were found unsearchable** (See Box I).

3. □ **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

□ the text is approved as submitted by the applicant.

☒ the text has been established by this Authority to read as follows:

METHOD FOR ENCRYPTING INFORMATION AND DEVICE FOR REALIZATION OF THE METHOD

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

□ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the drawings to be published with the abstract is Figure No. 1

□ as suggested by the applicant.

☒ because the applicant failed to suggest a figure.

□ because this figure better characterizes the invention.

□ None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/BY 99/00005

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 222 139 A (TAKARAGI ET AL.) 22 June 1993 (1993-06-22) column 2, line 55 - line 63 column 3, line 9 - line 27 column 8, line 41 - line 55	1,6

□ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 12 January 2000	Date of mailing of the international search report 20/01/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Holper, G

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/BY 99/00005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5222139 A	22-06-1993	JP 4170576 A	18-06-1992

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/06	A1	(11) International Publication Number: WO 00/65767 (43) International Publication Date: 2 November 2000 (02.11.00)

(21) International Application Number: PCT/BY99/00005

(22) International Filing Date: 27 April 1999 (27.04.99)

(71)(72) Applicant and Inventor: MISCHENKO, Valentin Alexandrovich [BY/BY]; 28–210, Nekrosova Str., Minsk, 220040 (BY).

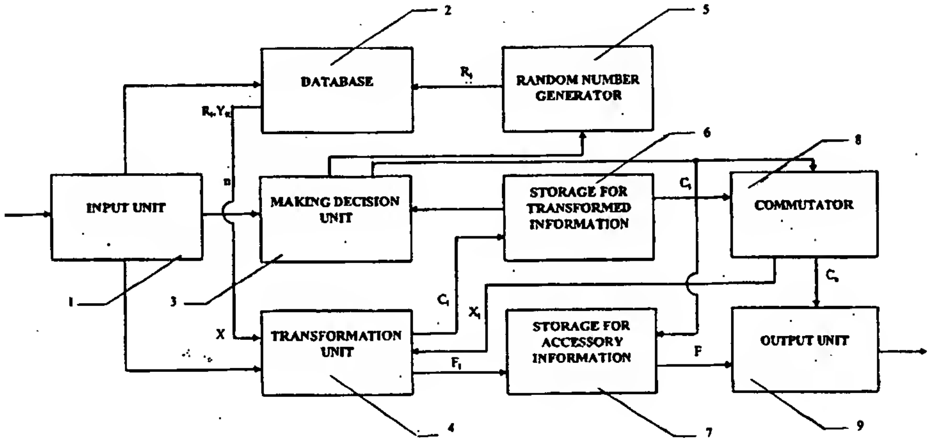
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: ZAKHARAU, Uladzimir Uladzimirovich [BY/BY]; 1–2–22, 50 Let Pobedy Str., Minsk, 220056 (BY). VILANSKI, Yuri V. [BY/BY]; 10–44, Kuleshova Str., Minsk 220026 (BY). VERZHBALOVICH, Dzmitry I. [BY/BY]; Mvizru Pvo, Minsk 220057 (BY).

(74) Agent: VINOGRADOV, Sergei Gennadievich; P.O. Box 261, Minsk, 220006 (BY).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD FOR ENCRYPTING INFORMATION AND DEVICE FOR REALIZATION OF THE METHOD



(57) Abstract

The invention relates to means for protecting information from an unauthorised access by electronic means. In order to transform the initial information the device has the transformation unit (4), the making decision unit (3), the storage of the recovered communication (6), the commutator (8), and for storing the accessory information the device has the storage of the accessory information (7). For encoding and transferring information the addressee is beforehand provided with a key to the received communications with information on regularities corresponding to the values of the communication transmitted to him, with specific values of the initial information for the whole set of symbols of the said kind of an information. In this case the addressee is beforehand provided with a set of transformation functions, Y_1, Y_2,..., Y_N = Y_i,(X), where X = {x_1, x_2,..., x_m} is a plurality of specific symbols of the transformed information. In the course of processing the encrypted information the input of the making decision unit (3) enters the information on the number (n) of transformation cycles of the initial communication. Before the beginning of the current transformation cycle, the making decision unit (3) transmits a control signal to the generator of random numbers (5), which generates a random number (Ri), transmits it to the data base (2) and through the latter to the transformation unit.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

INTERNATIONAL SEARCH REPORT

International Application No
PCT/BY 99/00005

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 222 139 A (TAKARAGI ET AL.) 22 June 1993 (1993-06-22) column 2, line 55 - line 63 column 3, line 9 - line 27 column 8, line 41 - line 55 -----	1,6

□ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 12 January 2000	Date of mailing of the international search report 20/01/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl	Authorized officer

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/BY 99/00005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5222139 A	22-06-1993	JP 4170576 A	18-06-1992

2/PRTS

IPC: G06K 9/62

METHOD OF ENCODING AND DECODING DATA AND DEVICE FOR REALIZATION OFTHE METHOD

The invention relates to means for protecting data from an unauthorized access, and may be used in crypto-systems for encoding, transferring and decoding communications, and in other systems for protection of data.

The prior art discloses engineering solutions providing protection of transmitted data by means of a special equipment or encoding software, for example by using scrambler for protection of telephone conversations [1] pp. 35-37, Fig. 22. The scrambler operates on the principle on inversion of an audio signal. As a result of an inversion a usual speech turns to a senseless gang of sounds, but the initial signal is accepted by the user without any distortion. The telephone set is equipped with the block for voice modification controlled by the encoder. The encoder stores 13122 user's codes providing 52488 digital combinations. The read-only memory of the set stores the resident software, which codes and decodes the transmitted data in several variants and controls the work of the whole set.

However this prior art solution has problems in providing a fair degree of secrecy, since for disclosing the confidential codes it is enough to execute a limited number of mathematical operations that are fast and effectively executed by the modern high-speed electronic engineering.

The main characteristic of a crypto-system is the degree of secrecy. The task of a cryptographer is to provide the utmost secrecy and authenticity of the transferred data. Alternatively, a crypto-analyst "forces open", or “breaks”, the crypto-system designed by a cryptographer. The crypto-analyst tries to decipher the set of encoded symbols and to deliver the encrypted communication as the plaintext.

Prior art discloses technical solutions for protecting the transferred data by using a specific device and/or encoding software. Known codes are based on two simple methods: substitution and interchange. Interchange uses simple mixing of plain-text symbols, the key of an interchange encryptor defines the specific type of mixing. The frequency distribution of individual symbols in the encoded text is identical to that of the plaintext. For substitution, each symbol of the plaintext is replaced by another symbol of the same alphabet, and the specific type of substitution is determined by the secret key.

For example, the algorithm in the Data Encryption Standard (DES) [2], p. 33-34 uses the both methods. The algorithm comprises plaintext, unencrypted text and the key as binary sequences having the length 64, 64 and 56 bits, respectively. When DES is used in an electronic book or table mode, the 64-bit blocks of the plaintext are encoded independently by using one key. The algorithm of DES includes 16 rounds or cycles, each of which has simple interchanges combined with substitution in four-bit groups. In each pass, 48 key bits are selected in a pseudo-random manner from the full 56-bit key.

The problem of DES is that this prior art solution does not provide a fair degree of secrecy, since for disclosure of such secret codes with possible number of 2^{64} keys combinations, substituting of all keys during a brute-force attack using modern computer techniques is performed in an acceptable time. Also, using the same plaintext and not varying the keys, produces the same encoded text. Analysis reveals the statistical regularity of the correlation between the plaintext and the encoded text, and may allow decoding the encoded text without using direct substitution of all the keys.

A crypto-system using public keys RSA is described in [2] p. 37-39. This system uses a one-way function - discrete logarithms raising to a power.

GOST P. 34.11 - 94 [3], p. 3-8 discloses hatching consisting in comparing an optional set of data as a sequence of binary symbols, with a short, fixed length image thereof. In this system 64-bit subwords are encoded using keys of 256 bit length.

The drawbacks of these systems are small the key length, which may permit decoding during acceptable time, and a slow decoding speed. These systems are practically stable systems.

Theoretically stable systems have perfect secrecy. According to Shannon [4] p. 333-402, that means that the plaintext, and the encoded text or cryptogram, are statistically independent for all plaintext and cryptograms.

A prior art Vernan crypto-system is a theoretically stable crypto-system. Theoretically stable systems make certain demands on a key. For a system with closed keys the indeterminacy of the key should not be less than the indetermina[illegible]f the plaintext. In theoretically s[illegible] systems the length of a key should be not less than the length of the plaintext. In the Vernan system the key length is equal to the length of the plaintext. This system was used in a code-notebook [5] for transfer of one encoded text. This is the main drawback of a codebook because the key should be changed and delivered with every transfer.

There are known crypto-systems using the so-called randomisers [2] p. 26 - 27. A randomiser is a software or a hardware device that encodes some symbols of plaintext with some random plurality of codes.

Typically, this is done for providing equal frequency of the plaintext alphabet. Symbol frequency equalisation is required so that a crypto-analyst cannot organise decoding of a plaintext based on analysis of frequency characteristics of a cryptogram. For a random plaintext and a random selection of a code, a derandomiser should correctly determine the initial symbol without transfer of data from the randomiser location. In classical systems with a small randomising field, this task is solved by substituting codes belonging to the randomised symbol. Randomisers, however, do not play a substantial role in crypto-protectability of an encoding system, as secret keys are the main means of protection.

Under the combination of the essential features the most close prior art object to the claimed method and device is the disclosed in [6] the device and method of encoding that use a principle of full randomizing symbols of the initial alphabet on a plurality of codes with potencies of large dimensionality, The said prior art invention was selected by the inventors for the prototype of the claimed invention.

In respect of a method the selected for the prototype object is a method of encoding and transferring data, wherein the addressee is beforehand provided for a key to the received communications with data on regularities corresponding to the values of the communication transmitted to him, with specific values of the initial data for the whole set of symbols of the said kind of an data, processing an data using the said regularities and transferring to the addressee the communication containing data, obtained during processings data, the values of transmitted data, which depend on random generated numbers being calculated during processing data, characterized in that the addressee is beforehand provided with a set of functions $Y_1 \ldots Y_n = Y_i(X)$, where X is a variable, and each Yi corresponds to a specific symbol of data, and also with the support function U = U

(Z), where Z is a variable, and with the key function W = W (Y, U), where Y and U are variables accepting values of any of the values from the values of the said functions Yi and U, in the course of processing of a transmitted data for each symbol there are generated two random numbers X and Z, the respective value of Y is calculated on basis of the respective function Yi (X) for a specific symbol, the value of U is further calculated on basis of the support function U (Z), the value of W for this symbol is calculated on basis of the key function W (Y, U) and obtained for the symbol value of Y and the value of U from the support function, and the addressee is transmitted the communication containing data on the thus obtained values of W, X and Z for each symbol of the initial data.

In respect of a device, the object selected for the prototype is a device for realizing a method of encoding and transferring data, which comprises a unit for data input, a set of symbols, a data base on plurality of characteristic functions that transform the specific symbols with the communication, which data base is supplied with a calculator connected to the generator of random numbers, the device further comprising the encoder and the unit for recording and transmitting communications, and the encoder being connected to the set of symbols and calculator output, the device further comprising a unit for calculating the values of the support function and a unit for calculating the values of the key function, the generator of random numbers is supplied with two outputs joint with the encoder, the first output of the generator of random numbers is connected also to the input of the unit for calculating values of the support function, and second – to the input of the calculator of the data base on regularities, the output of this calculator is connected to the encoder through the unit for calculating values of the key function, and the second input of the latter is connected to the output of the unit for calculating values of the support function.

However the problem of object selected for the prototype is that in the course of the encryption the length of the encrypted communication exceeds the length of the initial communication by several times.

The aim of the claimed invention is providing an improved method of encrypting by means of obtaining several communications from one initial, at least one of the obtained communications may be compressed up to preset sizes so that any connection between the initial text and the cryptogram is completely is lost for a cryptoanalyst.

As a result of the solution of the problem there is achieved a new technical effect consisting in creating a new system of encrypting that ensures a high crypto-stability of a system without any increase of the length of the communication. The said technical effect is achieved as follows.

The method of encrypting of an data comprises the following steps:

- Preliminary generation of data on plurality of characteristic functions that transform the values of symbols of the initial communication with the specific values of the encrypted communication for the total set of values of the said kind of communications;
- determination the number (n) of transformation cycles of the initial communication;
- realization of the transformation cycle comprising:
- generation of the feature (Ri), defining regularity used for transformation of the communication in the current transformation cycle;
- transformation of the communication with use of the selected regularity;
- repetition of transformation cycles the certain number of times;
- transformation of the communication in each cycle being realized in a way resulting in forming a communication (Ci), transformed in the said cycle and the accessory data for the said cycle (Fi);
- the number (n) of transformation cycles of the initial communication is selected from the preset criterion,
- forming the encrypted communication consisting of two parts, one of which contains the finally transformed communication (Cn), and second one contains a set of the accessory data (F = {F1, F2, ..., Fn}).

The further improvement of the method is characterized by that:

- transformation of the communication in each cycle is realized in a way resulting in forming a communication (Ci) transformed in the said cycle, being of the shorter or equal length with the initial communication, and resulting in forming an accessory data for the said cycle (Fi);
- the number (n) of transformation cycles of the initial communication is selected from the preset criterion (for example, the size of the finally transformed communication),
- forming the encrypted communication consisting of two parts, one of which contains the finally transformed communication (Cn) being of the shorter length

with the initial communication, and second one contains a set of the accessory data (F = {F1, F2, ..., Fn}).

Still further improvement of the method is characterized by that:

- transformation of the communication in each cycle realizes in a way resulting in forming a communication (Ci) transformed in the said cycle, being of the shorter, equal or longer length with the initial communication, and resulting in forming an accessory data for the said cycle (Fi);
- the number (n) of transformation cycles of the initial communication is selected from the preset criterion (for example, the size of the finally transformed communication),
- forming the encrypted communication consisting of two parts, one of which contains the finally transformed communication (Cn) being of the shorter, equal or longer length with the initial communication, and second one contains a set of the accessory data (F

The further improvement of a method is characterized by that in each or some cycles the communication (Ci) transformed in the said cycle and (or) an accessory data for the said cycle (Fi) are intermixed.

The following improvement of the method is characterized by that in each or some cycles of transformation the certain part of an accessory data for the said cycle (Fi) is added into the transformed in the said cycle communication (Ci). The structural interpretation of stated ideas could be considered on an example of the claimed device.

The device for a realizing the method of encrypting data comprises:

- an input unit,
- an output unit, the first input of which is connected to the second output of the commutator, and the second — to the output of the accessory data storage ;
- data base on the plurality of characteristic functions that transform the initial data with the encoded data, the first input of the said data base being connected to the first output of the input unit and the second input – to the output of the random numbers generator;
- a random number generator, the input of which is connected to the first output of the making decision unit;

- the transformation unit, the first input of which is connected to the second output of the output unit, the second input – to the output of the data base, and the third input –to the first output of the commutator;
- the storage for the transformed data, the input of which is connected to the first output of the transformation unit;
- a storage for the accessory data, the first input of which is connected to the second output of the transformation unit, and the second input – to the second output of the making decision unit;
- the making decision unit, the first input of which is connected to the third output of the input unit, the second input – to the first output of the storage for the transformed communication;
- the commutator, the first input of which is connected to the second output of the storage for the transformed communication, and the second input – to the second output of the making decision unit.

Another method of decoding encrypted data comprises the following steps:

- preliminary generating data on plurality of characteristic functions that transform values of all encoded symbols that may be used in the said kind of data with initial symbols, which are identical to the regularities used at encoding;
- extracting, from the encoded communication, of the data (R_i), defining the regularity which is used in the current transformation cycles and connects the values of the encoded communications with the concrete symbols of the transformed data of the current transformation cycle;
- selecting the regularity connecting the values of the encoded communications with the concrete symbols of the transformed data of the current transformation cycle;
- extracting from the accessory data (F) the accessory data for the said transformation cycle (F_i);
- transforming the transformed data (C_i) using the selected regularity and the accessory data for the said transformation cycle (F_i);
- making decision on switching to the next cycle or termination of the transformation;
- the accessory data for the said transformation cycle (F_i); being isolated from the array of the accessory data (F);

- recovering the data (C_i), which is transformed in the respective cycle, by using the selected regularity and the accessory data for the said transformation cycle (F_i);
- making decision on switching to the next cycle or termination of the transformation;
- using additionally in each transformation cycle a respective part of the accessory data, as a result of transforming with the use of the selected regularity there is formed the data recovered in the respective cycle.

The further improvement of a method is characterized by that:

- in each transformation cycle there is additionally used a respective part of the accessory data and as a result of the transformation with use of the selected regularity there is formed a recovered in the corresponding cycle communication, the length of which is larger or equal to the length of the communication, resulting from transforming in the previous cycle.

The following improvement of a method is characterized by in each transformation cycle there is additionally used a respective part of the accessory data, and as a result of transformation with use of the selected regularity there is formed a recovered in the respective cycle communication, the length of which is larger, equal or smaller than the length of the communication, resulting from transforming in the previous cycle.

One more improvement of the method is characterized by that the transformed in the respective cycle data (C_i) and/or the accessory data for the respective cycle (F_i) is preliminary unmixed in each cycle or in some cycles;

The device for realizing the method of decoding of the communication, comprises:

- an input unit (10),
- an output unit (15),
- data base on the plurality of characteristic functions that transform the encoded data with the initial data (2),
- a transformation unit (12);
- a storage of the transformed data (14) ;
- a storage of the accessory data (13);
- a making decision unit (11);
- a commutator (8),

the first inpu[illegible]the accessory data storage (13)[illegible]g connected with first output of the input unit (10) and the second input of the accessory data storage (13) being connected with first output a making decision unit (11); the first input of data base (2) is connected to the second output of the of the input unit (10), and the second input – to the first output of the storage for accessory data(13); the first input of the storage of the recovered data is connected to the third output of the input unit, the second – to the output of the transformation unit, and the third – to the first output of the making decision unit, the first input of the transformation unit is connected to the second output of the storage of accessory data, and the second – to the output of database, the third to the first output of the storage of recovered data; the second - to the fourth output of the input unit, the first input of the commutator is connected to the second output of the making decision unit, and the second – to the second output of the making decision unit, the output unit is connected to the second commutator output .

With the first output (exit) of the switchboard; the first input (entrance) of the block of a decision making is connected to the first output (exit) of an accumulator of the restored communication, and second — With the fourth output (exit) of the block of input; the first input (entrance) of the switchboard is connected to the second output (exit) of the block of a decision making, and second — With the second output (exit) of an accumulator of the restored communication; the block of a conclusion is connected to the second output(exit) of the switchboard.

The distinctive feature of the new method can be illustrated by the following example. Symbols of the initial alphabet A {a1, a2, ..., an} being such, that the binary representation of each symbol has the identical length for the whole alphabet A, are substituted with symbols of the alphabet Bi {b1i, b2i, ..., bni} being such, that the binary representation of each symbol may have a various length, the process of such replacement is iterative, i. e. at each i-step for the initial communication there is used a result of the substitution obtained at the i-1step, at each i-step there is used its own substitution alphabet Bi, produced with the help of the function Yi, selected by a casual mode from a plurality of functions transferred to the addressee beforehand, and at each i-step there is produced the accessory data Fi used for restoring the initial communication is produced. As an additional measure of protecting from cryptanalysis, on each step or on some steps there may be performed intermixing of the communication resulting from the transformation. In an outcome of such transformation there is produced a transformed text (Cn), length of which may be not than the less length of one symbol of the alphabet Bn, used at the last step of transformation.

Such systems have uncommon properties:

- as a result of transformation of the initial communication there are produced at least two output communications (the transformed communication (Cn) and the accessory data (F), each of which separately has not any sense from the point of view of restoring the initial communication and may be transmitted through a separate data link;
- generally, the length of the transformed communication may have the length of one symbol of the substitution alphabet, for example if the initial communication has the byte representation, the transformed communication may have the one byte length, regardless of the length and kind of the initial communication;
- at multiple encoding one and the same initial communication the transformed communication will be various, eliminating thereby a problem of the closed channel for the key data transfer;
- The modification of ay symbol in the transformed communication or accessory data brings about the impossibility of restoring the initial communication.

The transformation functions (Yi) may be preset in the form of a table. For example, in case of representing the initial communication as N-bit binary sequences and transformation of compression of the function Yi, can be preset as a set of 2^N triples — {(ak, bik, fik)}, where ak is an N-bit initial code, bik is a transformed bit code of a variable length not greater N, and only two values of {bik} have the length of N bit, fik is the data on the length of the respective bik in bits. At such representation there exist such submission exist $(2^N)!(2^N-1)(2^N-2)$ of various possible functions of transformation such, that $\sum_{i=1}^{2^N} L_{ik} = \min L_{ik}$, where - L_{ik} - is length of bik in bits. At N = 8 there is present ≈256! *254*255 10^{511} of various transformation functions (Yi). In this case two values of bik have the one bit length, four values of bik have the two bit length, eight values of bik have the three bit length, sixteen values of bik have the four bit length, a thirty two values of bik have the five bit length, sixty four values of bik have the six bit length, one hundred twenty eight values of bik have the seven bit length and two values of bik have the eight bit length.

Then [illegible] an arbitrary function Yi the av[illegible]e length of the transformed communication X will be equal:

$$\mathrm{L}(\mathrm{C}_i(\mathrm{X},\mathrm{Y}_i)) = \mathrm{L}(\mathrm{X})\frac{2\mathrm{N}+\sum_{n=1}^{N-1} n2^{n}}{N2^{N}}$$

and the average length of an accessory data:

$$\mathrm{L}(\mathrm{F}_i(\mathrm{X},\mathrm{Y}_i)) = \mathrm{L}(\mathrm{X})\frac{2\mathrm{N}+\sum_{n=1}^{N-1} n2^{N-n}}{N2^{N}}$$

thus the average compression ratio at one step of transformation will have the values:

$$\mathrm{K}_{\mathrm{core}} = \frac{\mathrm{L}(\mathrm{C}_i(\mathrm{X},\mathrm{Y}_i))}{\mathrm{L}(\mathrm{X})} = \frac{2\mathrm{N}+\sum_{n=1}^{N-1} n2^{n}}{N2^{N}}$$, for the transformed communication

$$\mathrm{K}_{\mathrm{flags}} = \frac{\mathrm{L}(\mathrm{F}_i(\mathrm{X},\mathrm{Y}_i))}{\mathrm{L}(\mathrm{X})} = \frac{2\mathrm{N}+\sum_{n=1}^{N-1} n2^{N-n}}{N2^{N}},$$ for the accessory data.

In particular, for N = 8 we have: $\mathrm{K}_{\mathrm{core}} = 777/1024$ 0.758 $\mathrm{K}_{\mathrm{flags}} = 255/1024$

At performing transformation M cycles the anticipated average length of the transformed communication will be:

$$L(C(X)) = K_{core}^{M} L(X),$$

and of the accessory data -

$$L(F(X)) = L(X)K_{flags}\sum_{m=0}^{M-1} K_{core}^{m} = K_{flags}L(X)\frac{K_{core}^{M}-1}{K_{core}-1} \quad .$$

Accordingly at performing 10 transformation cycles the average length of the transformed communication at of N = 8 will make approximately 0,067 of the length of the initial communication, and length of the accessory data — 0.97 of the length of the initial communication. The general length will make approximately 1.037 of the initial length, and for 100 transformation cycles — 10^{-12} and 1.04 accordingly.

If at each transformation cycle a S byte of the accessory data is added to the transformed communication, then average length of the transformed communication will be:

$$L(C(X)) = K_{core}^{M} L(X) + S\sum_{m=0}^{M} K_{core}^{m} = K_{core}^{M} L(X) + S\frac{K_{core}^{M+1}-1}{K_{core}-1},$$

And length of an accessory data will make:

$$L(F(X)) = \sum_{m=1}^{M} K_{flags}\left(K_{core}^{m} L(F) + S\frac{K_{core}^{m+1}-1}{K_{core}-1}\right) = \frac{K_{flags}}{1-K_{core}}\left(L(X)(1-K_{core}^{M}) + S\left(M - \frac{K_{core}^{M+2}-1}{K_{core}-1}\right)\right)$$

The construction of the claimed device may be realized in various variants realizing the claimed method of encoding data by using the known hardware. All these variants expand technological possibilities of using of the invention.

The main problem of the prototype method is eliminated thereby, i.e. essential increase of the sizes of the encrypted communication in a comparison with the initial one. The disclosed distinctive features of the claimed invention, in a comparison with known engineering solutions allow designing a device of encoding data providing statistical independence of the encrypted text and the open text, i.e. having properties of the theoretically stable of proof system of cryptography, and not by recurrence of the encrypted communication at repeated encoding of one and the same communication at constant keys.

Fig.1 shows a diagram of the device illustrating realization of a claimed method of encoding data is represented. Through the input unit the data base enters the pre- generated data on plurality of characteristic functions that transform values of symbols of the initial communication with specific symbols of the encrypted communication for the whole set of symbols of the said kind of the communications. In the course of processing the encrypted data the input of the making decision unit (3) enters the data on the number (n) of transformation cycles of the initial communication. Before the beginning of the current transformation cycle, the making decision unit (3) transmits a control signal to the generator of random numbers (5), which generates a random number (Ri), transmits it to the data base (2) and through the latter- to the transformation unit. In accordance with the value of Ri from the database (2) there is selected the transformation function of YRi which enters the transformation unit (4). The transformation unit (4) calculates s the values of (Ci, Fi) = YRi (Xi, Ri). The value of Ci enters the input of the storage of the transformed communication (6) from outputs of the transformation unit (4) and the value of Fi enters the input of the storage of the accessory data (7). The storage of the transformed communication (6) transmits a signal on termination of the current cycle of transformation to the making decision unit (3). The making decision unit (3) makes a decision on fulfillment of the next transformation cycle or on terminating the process of transformation. In case of decisionmaking on the terminating the process of transformation the transformed data (Cn) through the switchboard (8) and the accessory data F = {F1, F2, ..., Fn} from the storage of an accessory data (7) enters the output unit (9). Otherwise the transformed communication (Ci) through the switchboard (8) enters in the transformation unit (4) for fulfillment the next cycle of transformation.

Fig. 2 shows the diagram of the device illustrating realization of the claimed method of decoding data. Through the input unit (10) into the data base (2) come the previously generated data on plurality of characteristic functions that transform values of symbols of the initial communication with special symbols of the encrypted communication for the whole set of symbols of the said kind of the communications, which are identical to the regularities used at encoding. In the course of restoring the transformed communication through the input unit (10) enter the following data: at the input of the decision making unit (11) - data on the number (n) of transformation cycles of the deencrypted communication; at the storage of the accessory data (14) – the accessory data; at the storage of the restored communication (13) – the transformed communication. Before the beginning of the current cycle of restoring at the signal of the decision making unit (11) the storage of the accessory data (14) yields the accessory data (Fi) into the transformation unit (12) and the value of Ri – into the data base (2), in accordance with which is selected the function of transformation of Yri that arrives at the transformation unit (12), and the storage of the restored communication (13) yields through the switchboard (8) the transformed communication (Ci) into the transformation unit (12). The transformation unit (12) calculates the values of (Xi)) YRi (Ci, Fi). From the output of the transformation unit (12) the restored communication (Xi)) arrives into the storage of the restored communication (13). At completion of accumulation of the restored communication (Xi)) the storage of the restored communication (13) sends a signal on termination of the current cycle of restoring into the decision making unit (11). In case of decision-making on the termination of process of transformation the restored communication (Xi)) through the switchboard (8) arrives to the output unit (15). Otherwise from the output of the decision-making unit (11) at the input of the storage of the accessory data (14) arrives the signal on yielding of the next portion of the accessory data (Fi, Ri) and the restored communication arrives through the switchboard (8) at the transformation unit (12) for fulfillment of the next cycle of restoring.

Bibliographic data of sources of data

1. Victor Gavrish "Practical Guide on Protecting Commercial Secrets". Simferopol, TAVRIDA, 1994, p.35-37.
2. . Schmidt M. E., Bransted D.K. "Standard of Data Encoding: Past and Future" Journal of Works of Electronic and Radio Engineers (TIIER), 1988, v.76, no. 5., p. 33-34.
3. GOST 34.11-94 Data Technology, Crypto Graphical Protection of Data, Cash function. M.: Gosstandart of Russia, 1994, 34.11 - 94, p. 3-8.
4. Shannon C. E.. "Communication Theory in Secret Systems". Shannon C. E. "Works on Data and Cybernetics Theory". M.: IL, 1963, p. 333-402, “Theoretically Stable system,”, as cited in “An Introduction to Contemporary Cryptology”, Proceedings of the IEEE, v. 76. No. 5, May 1998.
5. Vernan. Copher printing telegraph systems for secret wire and radio telegraphic communications. // J Amer. Inst. Elec. Eng., vol. 55, pp. 109-115, 1926.
6. Mischenko V.A, Zakharov V.V. A method of encoding and transfer data and the device for a realization the method // Official Gazette of the Belarusian Patent Office. No.4, part I, 1997
7. Golubev V.V. Computer crimes and protection of data in computing systems // News in life, science and engineering. Part. Computer engineering and use thereof. Protection of data.- M.: Znanie, 1990.

Claims

1. A method for encoding data comprising the steps of:

- preliminary generating data on plurality of characteristic functions that transform values of initial information of a full set of symbols into encoded data;
- determining the number (n) of cycles of transforming specific initial data;
- realising the cycle of transforming which comprises:
- generating the feature (R_i) that determines the regularity used for transforming the data in the current transformation cycle;
- transforming the data using the selected regularity;
- repeating transformation cycles a certain number of times;

- *characterised in that,*
- transforming of the data in each cycle is performed in such a way that results in forming a transformed in the said cycle data (C_i) and the accessory data for the said cycle (F_i);
- the number (n) of cycles of the transformation of the initial data is selected from the preassigned criterion,
- forming an encoded message consisting of two parts, one of the said parts comprises the finally transformed data (C_n), and the second one comprises the accessory data array ($F = \{F_1, F_2, \ldots, F_n\}$).

2. The method for encoding data according to claim 1, *characterised in that*

- transforming the data in each cycle is performed in such a way that results in forming a transformed in the said cycle data (C_i), that is shorter or equal to the length of the initial data, and the accessory data for the said cycle (F_i);
- the number (n) of cycles of the transformation of the initial data is selected from the preassigned criterion determining the size of the finally transformed data,
- forming an encoded message consisting of two parts, one of the said parts comprises the finally transformed data (C_n) that is shorter than the length of the initial communication, and the second one comprises the accessory data array ($F = \{F_1, F_2, \ldots, F_n\}$).

3. The method for encoding data according to claim 1, *characterised in that*

- transforming the data in each cycle is performed in such a way that results in forming a transformed in the said cycle data (C_i) that is shorter, equal or longer than the length of the initial data and the accessory data for the said cycle (F_i);

- the numb[illegible]n) of cycles of the transformation[illegible]he initial data is selected from the preassigned criterion, determining the size of the finally transformed data and/or the degree of protectability of data,
- forming an encoded data consisting of two parts, one of the said parts comprises the finally transformed data (C_n) that is shorter, equal or longer than the length of the initial communication, and the second one comprises the accessory data array ($F = \{F_1, F_2, \ldots, F_n\}$).

4. The method according to claims 1, 2 or 3, *characterised in that* the transformed in the said cycle data (C_i) and/or the accessory data for the said cycle (F_i) are mixed in each cycle or in some cycles.
5. The method according to claims 1, 2, or 3, or 4, *characterised in that* the certain part of the accessory data for the said cycle (F_i) is added to the transformed in the said cycle data (C_i) in each or some transformation cycles.
6. The device for realising the method for encoding of data, comprises:

- an input unit,
- an output unit, the first input of which is connected with the second output of the commutator, and the second — with the output of the accessory data storage ;
- data base on the plurality of characteristic functions that transform the initial data with the encoded data, the first input of the said data base being connected with the first output of the input unit and the second input – with the output of the random numbers generator;
- *characterised in that*, the device further comprises
- a random number generator, the input of which is connected with the first output of the making decision unit;
- the transformation unit, the first input of which is connected with the second output of the output unit, the second input –with the output of the data base, and the third input –with the first output of the commutator;
- the storage for the transformed data, the input of which is connected with the first output of the transformation unit;
- a storage for the accessory data, the first input of which is connected with the second output of the transformation unit, and the second input – with the second output of the making decision unit;
- the making decision unit, the first input of which is connected with the third output of the input unit, the second input – with the first output of the storage for the transformed communication;

- the comparator, the first input of which is connected with the second output of the storage for the transformed communication, and the second input – with the second output of the making decision unit.

7. The method for decoding of the encoded data comprising the steps of:

- preliminary generating data on plurality of characteristic functions that transform values of all encoded symbols that may be used in the said kind of data with initial symbols, which are identical to the regularities used at encoding;
- extracting , from the encoded communication, of the data (R_i), defining the regularity which is used in the current transformation cycles and connects the values of the encoded communications with the concrete symbols of the transformed data of the current transformation cycle;
- selecting the regularity connecting the values of the encoded communications with the concrete symbols of the transformed data of the current transformation cycle;
- extracting from the accessory data (F) the accessory data for the said transformation cycle (F_i);
- transforming the transformed data (C_i) using the selected regularity and the accessory data for the said transformation cycle (F_i);
- making decision on switching to the next cycle or termination of the transformation;
- *characterised in that,* the accessory data for the said transformation cycle (F_i); is isolated from the array of the accessory data (F);
- recovering the data (C_i), which is transformed in the respective cycle, by using the selected regularity and the accessory data for the said transformation cycle (F_i);
- making decision on switching to the next cycle or termination of the transformation;
- using additionally in each transformation cycle a respective part of the accessory data, as a result of transforming with the use of the selected regularity there is formed the data recovered in the respective cycle.

8. The method of decoding the encoded data according to claims 7, *characterised in that*

- in each transformation cycle there is additionally used a respective part of the accessory data and as a result of transformation with use of the selected regularity there is formed a recovered in the corresponding cycle communication, the length of which is larger or equal to the length of the communication, resulting from transforming in the previous cycle.

9. The method of decoding the encoded data according to claims 7, *characterised in that*

in each transformation cycle there is additionally used a respective part of the accessory data, and as a result of transformation with use of the selected regularity there is formed a recovered in the respective cycle communication, the length of which is larger, equal or smaller than the length of the communication, resulting from transforming in the previous cycle.

10. The method according to claims 7, 8 or 9, *characterised in that*, the transformed in the respective cycle data (C_i) and/or the accessory data for the respective cycle (F_i) is preliminary unmixed in each cycle or in some cycles;

11. The device for realising the method for decoding data, comprises:

- an input unit,
- an output unit,
- data base on the plurality of characteristic functions that transform the encoded data with the initial data,
- *characterised in that*, the device further comprises
- a transformation unit;
- a storage of the recovered communication;
- a storage of the accessory data;
- a making decision unit;
- a commutator,

the first input of the accessory data storage connected with first output of the input unit and the second input of the accessory data storage connected with first output a making decision unit; the first input of data base is connected to the second output of the of the input unit, and the second input – to the first output of the storage for accessory data; the first input of the storage of the recovered data is connected to the third output of the input unit, the second – to the output of the transformation unit, and the third – to the first output of the making decision unit, the first input of the transformation unit is connected to the second output of the storage of accessory data, and the second – to the output of database, the third to the first output of the storage of recovered data; the second - to the fourth output of the input unit, the first input of the commutator is connected to the second output of the making decision unit, and the second – to the second output of the making decision unit, the output unit is connected to the second commutator output .

(11) **WO 0[illegible]767**
(21) PCT/B[illegible]9/00005
(22) **27 April 1999 (27.04.1999)**
(25) ENG
(43) 02 November 2000 (02.11.2000)
(51)[7] H04L 9/06
(54) METHOD FOR ENCRYPTING INFORMATION AND DEVICE FOR REALIZATION OF THE METHOD

(71)(72) **MISCHENKO, Valentin Alexandrovich** 28-210, Nekrasova Str., Minsk, 220040 ; (BY). [BY/BY].
(72)(75) **ZAKHARAU, Uladzimir Uladzimirovich** 1-2-22, 50 Let Pobedy Str., Minsk, 220056 ; (BY) [BY/BY].
VILANSKI, Yuri V. 10-44, Kuleshova Str., Minsk 220026 ; (BY) [BY/BY].
VERZHBALOVICH, Dzmitry I. Mvizru Pvo, Minsk 220057 ; (BY) [BY/BY].

Abstract

The invention relates to means for protecting information from an unauthorised access by electronic means. In order to transform the initial information the device has the transformation unit (4), the making decision unit (3), the storage of the recovered communication (6), the commutator (8), and for storing the accessory information the device has the storage of the accessory information (7). For encoding and transferring information the addressee is beforehand provided with a key to the received communications with information on regularities corresponding to the values of the communication transmitted to him, with specific values of the initial information for the whole set of symbols of the said kind of an information. In this case the addressee is beforehand provided with a set of transformation functions, Y 1 , Y 2 ,..., Y N = Y i ,(X), where X = {x 1 , x 2 ,..., x m } is a plurality of specific symbols of the transformed information. In the course of processing the encrypted information the input of the making decision unit (3) enters the information on the number (n) of transformation cycles of the initial communication. Before the beginning of the current transformation cycle, the making decision unit (3) transmits a control signal to the generator of random numbers (5), which generates a random number (Ri), transmits it to the data base (2) and through the latter to the transformation unit.

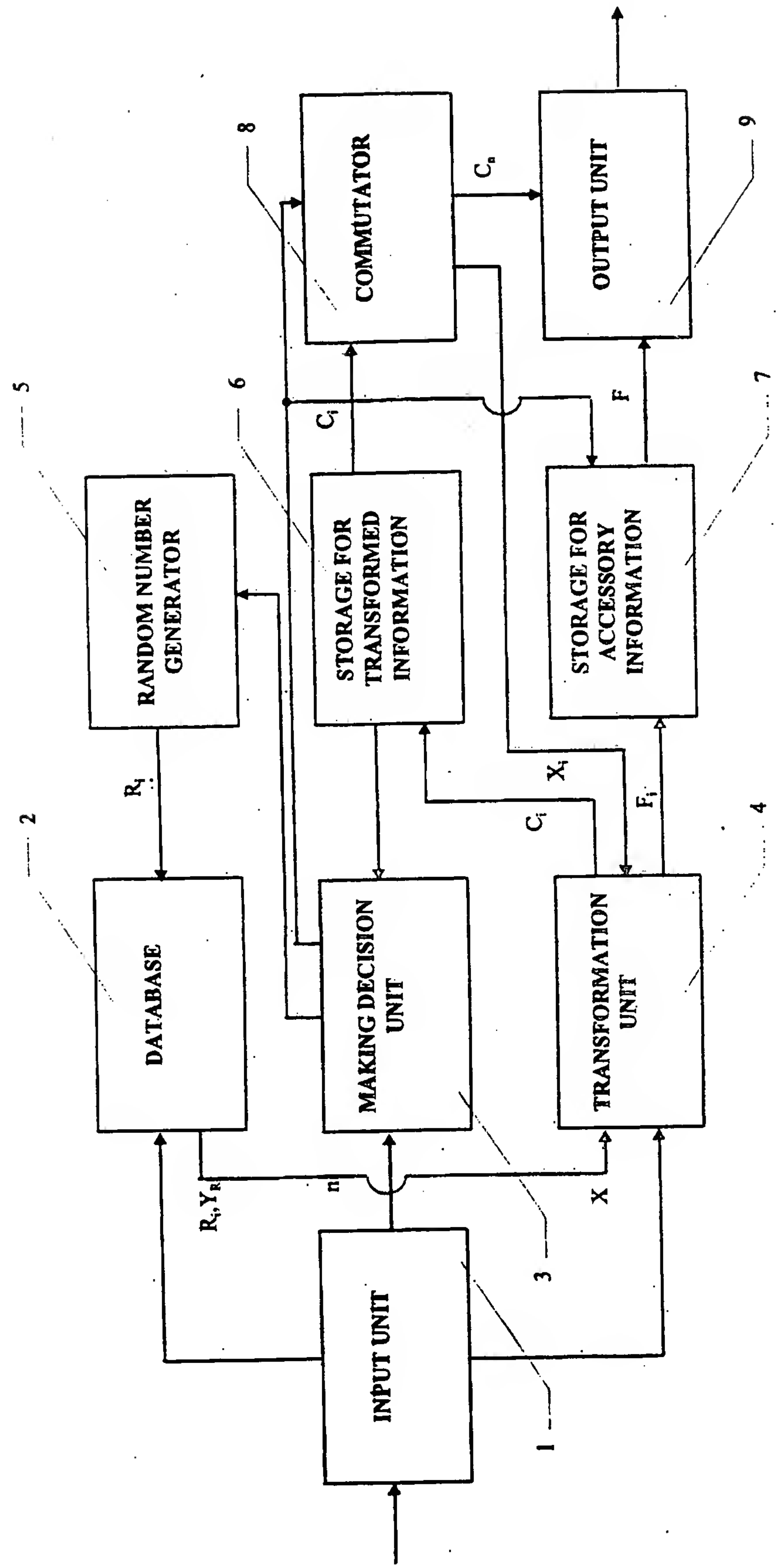

INPUT UNIT
DATABASE
MAKING DECISION UNIT
TRANSFORMATION UNIT
RANDOM NUMBER GENERATOR
STORAGE FOR TRANSFORMED INFORMATION
STORAGE FOR ACCESSORY INFORMATION
COMMUTATOR
OUTPUT UNIT
1
2
3
4
5
6
7
8
9
R_i, Y_R
n
X
R_q
C_i
X_i
F_i
C_i
F
C_n

FIG 1

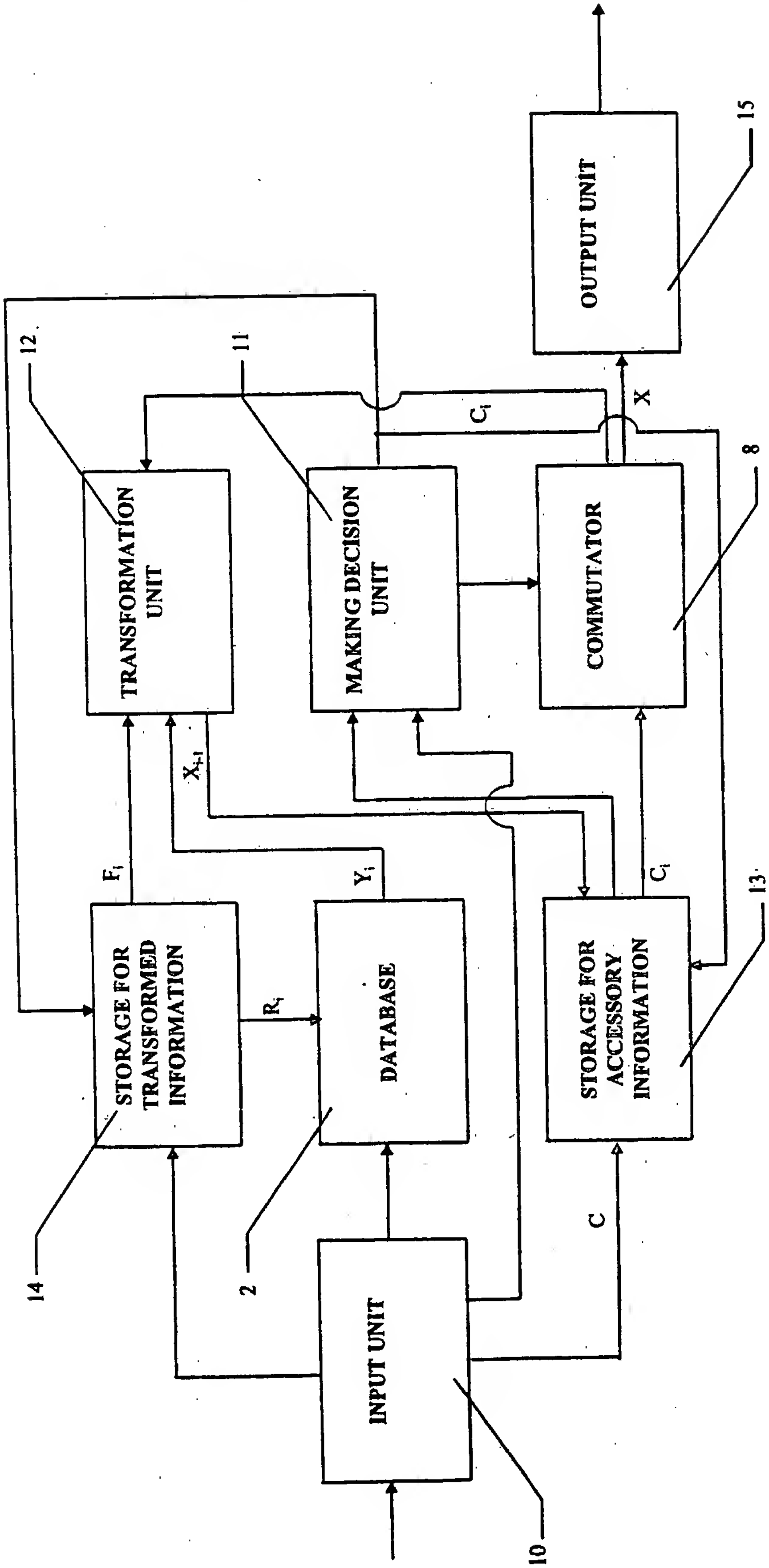

INPUT UNIT
DATABASE
STORAGE FOR TRANSFORMED INFORMATION
STORAGE FOR ACCESSORY INFORMATION
TRANSFORMATION UNIT
MAKING DECISION UNIT
COMMUTATOR
OUTPUT UNIT
F_i
R_i
Y_i
X_{i-1}
C_i
C_i
C
X
10
2
14
13
12
11
8
15

FIG. 2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/BY 99/00005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5222139 A	22-06-1993	JP 4170576 A	18-06-1992

INTERNATIONAL SEARCH REPORT

Interr   nel Application No
PCT/BY 99/00005

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7   H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7   H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic deta bese consulted during the international search (neme of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevent passages	Relevent to cleim No.
A	US 5 222 139 A (TAKARAGI ET AL.) 22 June 1993 (1993-06-22) column 2, line 55 - line 63 column 3, line 9 - line 27 column 8, line 41 - line 55 -----	1,6

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in ennex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of enother citation or other special reason (as specified)

"O" document referring to en orel disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of perticular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particuler relevance; the claimed invention cannot be considered to involve en inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 12 January 2000	Date of mailing of the internationel search report 20/01/2000
Name end mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Holper, G